IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

FOR:

SYSTEM AND METHOD FOR USING DRM TO CONTROL CONDITIONAL ACCESS TO DVB CONTENT

INVENTORS:
JUKKA ALVE
ARI IKONEN
MAURI KANGAS
TAPANI HEIKKILÄ

Morgan & Finnegan, L.L.P.
345 Park Avenue
New York, New York 10154-0053
(212) 758-4800
(202) 857-7887

Attorneys for Applicant

SYSTEM AND METHOD FOR USING DRM TO CONTROL CONDITIONAL ACCESS TO DVB CONTENT

Field Of The Invention

[0001] This invention generally relates to the protected transmission and use of digital video broadcast (DVB) content. More specifically it relates to secure DVB content delivery and rights management using a mobile terminal.

Background Of The Invention

[0002] DVB provides a standard for the distribution of digital broadcast video content. One of the issues concerning the adoption of DVB is that the pristine digital content provided by the standard could potentially be recorded and distributed without loss of quality and without the content owner's consent. To avoid unauthorized distribution the DVB standard includes a mechanism for encrypting the distributed content prior to transmission. DVB, however, does not dictate a digital rights management (DRM) scheme or key delivery standard. These two elements ensure the secure transmission and conditional access to the protected content. DVB leaves this aspect of content protection to the development of proprietary DRM systems.

[0003] In any rights managements system encryption of the delivered content is relatively simple. What is more difficult is distributing conditional access to the rights needed to decrypt and use the distributed information. Rights embody what an end user is allowed to do with the encrypted content, for example, play the content for a certain period or copy the content a limited number of times. DRM accomplishes this conditional access to the content by wrapping the keys required to decrypt the content into a tightly controlled system where the rights themselves cannot be freely copied or distributed, see Published U.S. Patent

Application No. 2003-0076955-A1. The successful control of these rights requires that they be individualized to restrict distribution of the rights beyond a particular authorized end user.

[0004] Current DVB DRM solutions transmit these rights as vouchers sent along with the same broadcast that carries the DVB transmission. This approach can be very wasteful of bandwidth because each user needs to receive an individualized rights voucher. As the number of vouchers grows the broadcast link's bandwidth, which must also carry the digital content, will be needlessly wasted. This method of voucher transmission is particularly wasteful because every user that receives the broadcast receives not only the voucher intended for that user but also the vouchers intended for every other user.

[0005] Other approaches to provide DRM control utilizing specialized equipment, such as set top boxes with smart cards and modems, to distribute rights vouchers through different communications links, for example over telephone lines. However, the specialized equipment required to carry out the rights delivery prevents over-the-air broadcasters from efficiently controlling an end user's equipment the way a cable distributor might. The problem is that while the over-the-air broadcasters would like to develop additional broadcast pay systems, they cannot without first developing a unified hardware infrastructure for the end users, including DRM infrastructure (hardware and software) and billing mechanisms. The investment required to create a system would be substantial for any one broadcast channel. Additionally end users would be unlikely to invest in or acquire new equipment for a system that worked for one only channel.

Summary Of The Invention

[0006] The above identified problems are solved and a technical advance is achieved in the art by providing a system and method for using DRM to control conditional access to DVB content.

[0007] An exemplary embodiment of the present invention includes a DRM system that encrypts a DVB service key and creates rights vouchers describing the rights associated with the use of the DVB service key. A rights voucher and the encrypted service key are sent to a mobile terminal, which is programmed to decrypt the service key in accordance with the rights articulated in the rights voucher. A DVB display device receives content encrypted with a content key and also receives a version of the content key that has been encrypted with the service key. The DVB display device sends the encrypted content key to the mobile terminal. The mobile terminal decrypts the content key with the service key in accordance with the rights defined in the rights voucher. The mobile terminal sends the decrypted content key to the DVB display device where it is used to decrypt the encrypted content.

[0008] In a further exemplary embodiment of the present invention, the DRM system sends the mobile terminal an executable application. The mobile terminal then runs the application which governs the service and content key decryption and enforces the assigned rights.

[0009] In a further exemplary embodiment of the present invention, the DRM system and the mobile terminal both operate according to the OMA DRM standard to protect the service key, define the rights voucher, and to enforce the granted rights on the mobile terminal.

[0010] In a further embodiment of the present invention the mobile terminal connects to the DVB display device via Bluetooth.

[0011] In a further embodiment of the present invention the mobile telephone billing system is used to bill for the use of DVB content.

[0012] Other and further aspects of the invention will become apparent during the course of the following description and by reference to the attached drawings.

Brief Description Of The Drawings

[0013] Figure 1 is a block diagram showing the delivery of DVB encrypted content.

[0014] Figure 2 is a block diagram showing an exemplary embodiment of the present invention disclosing a DRM system for DVB using a mobile terminal.

[0015] Figure 3 is a block diagram showing an exemplary embodiment of the present invention disclosing the operation of and communication between a mobile terminal and a DVB set top box.

Detailed Description

[0016] The system and method of the present invention provide an efficient and secure method for transmitting DRM rights in a DVB environment. The present invention has the advantage of using a separate distribution path to allow transmission and rights control to occur in a protected manner without needlessly wasting broadcast transmission bandwidth. Additionally, in a particularly advantageous embodiment the present invention employs the mobile telephone infrastructure and established mobile DRM standards for ready made billing and content control.

[0017] Figure 1 presents an overview of the DVB content encryption and delivery scheme. Clear, i.e. unencrypted, DVB content 1c is first encrypted in accordance with the DVB common scrambling algorithm (DVB CSA 5). DVB CSA 5 takes the clear DVB content 1c and a random CSA control word 10 as input. DVB CSA 5 then employs a symmetric encryption algorithm to generate the encrypted DVB content 1e. The CSA control word 10 must later be used by a decryption algorithm to decrypt the encrypted DVB content 1e and recover the usable clear DVB content. The CSA control word can, therefore, be thought of as the key to the distributed encrypted content. The encrypted DVB content 1e is now safe to freely broadcast over the airways 50 to DVB end users 40. With regard to the end users, the figures only show one symbol to designate end users 40, however, it should be understood that any number of end users might receive the broadcasted content. In addition, the identified end user 40 represents a number of hardware and software structures that perform DVB functions, e.g. receiving and decrypting DVB content and messages. The end user structures can be embodied by any suitable known equipment, such as TVs, tuners, or set top boxes programmed to operate in accordance with the DVB standard and the disclosed system.

[0018] The process described thus far is defined by the DVB standard and therefore should be consistent among various DVB implementations. However, the encrypted DVB content received by the end users 40 will only be useful if it can be decrypted. To do so, the end user 40 will require a copy of the CSA control word 10. The DVB standard, however, does not dictate how to securely transmit control words to end users. It also does not dictate how to ensure that the control words, once distributed, are only used in accordance with the rights dictated by the content providers. A complete DRM system must, therefore, both protect the secrecy of the control words in transit and limit their use by the end users in

accordance with the rights granted by the content providers. A general approach for carrying out this proprietary aspect of the DVB system is shown in the dashed rectangle in Figure 1.

[0019] First, the CSA control word 10 is encrypted 20 with a service key (SK 22). The service key is used to encrypt all CSA control words associated with a particular DVB service, e.g. a premium channel or a pay-per-view event. Different services, however, would most likely use different keys. The encrypted CSA control word is added to an entitlement control message (ECM 25). In addition to the encrypted CSA control word, the ECM 20 might also include header information or other relevant data. The ECMs are then transmitted over the broadcast network to the end users 40.

[0020] The encrypted CSA control word contained in the ECM must be decrypted before it can, in turn, be used to decrypt the encrypted DVB content. Accordingly, the service key SK 22 must be transmitted to the end user. To do so securely, the service key is encrypted 28 with a user key (UK 27) that is specific to a particular end user. Typically the UK is stored in a protected smart card in the end users set top box. The encrypted SK is then used to generate an entitlement management message EMM 29. The EMM might also include header or rights information. The transmitted rights information, for example, would dictate how the end user can use the protected content.

[0021] Unlike the previous encryption steps, the user key does not need to be transmitted to the end users 40 because the end users' hardware is pre-programmed to decrypt data encrypted with the users' UK. A number of procedures can be employed to ensure the secrecy and usability of the UK. For example, the end users' hardware can be pre-programmed with a shared secret known by the DVB system. Or, a public key cryptography system can be employed to encrypt the SK without ever knowing the end users' UK. In

either instance, upon receipt of EMM the end user decrypts the service key which in turn is used to decrypt the CSA control word which ultimately is used to decrypt the broadcast content.

[0022] As shown in Figure 2, the general approach for transmission of DVB content is modified to employ a mobile terminal 70. The delivery of the encrypted DVB content 1e and encrypted control words within ECMs 25 is done as shown in Figure 1. The introduction of a mobile terminal, however, allows the system of Figure 2 to off-load DRM implementation and service requirements from the DVB broadcaster to the mobile telephone/data network.

[0023] The content provider, i.e. the broadcaster, delivers the SK together with other data relating to the content, to the DRM system. In practice this could be accomplished by a server at the content provider generating and sending the SK via any known method of computer to computer communication.

[0024] In one embodiment, the SK is sent already encrypted by the UK in an EMM. The DRM system would add the particular formatting and rights information needed and then send the EMM to the Mobile terminal.

[0025] In an alternative embodiment, as shown in Figure 2, the broadcaster could provide the DRM System 30 with the SK prior to its encryption with a UK 27. This would limit the amount of data traffic between the DVB broadcaster and the DRM System 30 because the SK is generic to all users, while an encrypted EMM is user specific and must be generated for each end user requesting the service. These two examples demonstrate the fact that the various aspects of the DVB encryption/broadcast and the DRM System can be split

up between the DVB and DRM service providers in any number of ways, including a system where the DVB provider also performs the DRM services.

[0026] The rights enforcement supplied by the DRM System can be performed with any known DRM technique. For example, the mobile terminals participating in the system can be designed from the ground up to include a UK and DRM software and/or hardware that protects the UK. The software and/or hardware would ensure that the mobile terminal only uses the UK in accordance with instructions provided by the DRM system. In this embodiment, the DRM system would either need to know the UK, i.e. a shared secret, or know how to encrypt content so that the UK can decrypt it, i.e. public key cryptography.

[0027] Returning to the embodiment of Figure 2A, once the DRM System 30 receives the SK 22 it provides DRM protection for the SK and distributes it to the end users over the mobile telephone network. The DRM System can be embodied by a computer or a group of computers that are programmed to perform the disclosed operations and are connected to the mobile telephone network such that they can transmit data to mobile terminals.

[0028] The DRM System may also have data stored on the user, such as e.g. identification data (name, address, phone number), data relating to his DRM compliant devices, data relating to content subscription, data relating to billing etc. The DRM System may communicate with the mobile network operator, e.g. for billing purposes.

[0029] In the present embodiment one of the functions of the DRM System is to provide the DRM infrastructure to the mobile terminal 70. As shown in Figure 2, the DRM system provides the mobile terminal 70 with a Protected Application 36 containing the UK 27. The Protected Application runs on the mobile terminal and performs DRM operations, such as, e.g., key decryption and rights enforcement. The Protected Application can be

programmed according to any know methods of providing protected computing. Moreover, once installed in the mobile terminal the Protected Application provides DRM enforcement for any number of EMMs sent by the system. This embodiment is particularly advantageous because it provides for the delivery of the UK. It can, therefore, both initiate a mobile terminal that has never participated in the particular DRM system, and refresh the UK on mobile terminals in the system to provide updated security.

[0030] In addition to providing the Protected Application, the DRM System must also be programmed to provide a protected SK, and rights dictating its use, to the mobile terminal. This is accomplished by encrypting/wrapping 34 the SK to create an EMM wrapped in a DRM Voucher 35, which dictates the usage rights for the SK. Accordingly, the computers embodying the DRM System 30 are programmed to wrap and encrypt 34, i.e. encapsulate, the EMM and other data into a DRM Voucher 35. The DRM System 30 communicates with mobile terminals through a mobile network 80 to deliver the DRM messages and objects, e.g. DRM Voucher and Protected Applications.

[0031] As a rights object, the DRM Voucher could also include protected rights definitions dictating the number and type of uses that can be performed on the content associated with the SK. The DRM Vourcher may further comprise other data, e.g. data relating to the requested/ordered content and data relating to the billing or payment. The DRM Vourcher may be expressed in a rights expression language, such as e.g. ODRL, or in an extensible markup language such as e.g. XML or in any derivatives thereof.

[0032] The function of the rights object, however, could be implemented in a less flexible way by pre-programming the rights into the system or the protected application. For

example, the Protected Application could be programmed to only allow a certain set of rights, e.g. one play, for all EMMs it receives.

[0033] Turning now to the operation of the mobile terminal and the operations performed at the end user 40. As noted above, the end user 40 employs a means of receiving DVB encrypted content and providing output via a display. In the disclosed embodiment this operation is performed by a DVB set top box, however, the disclosed operations can be integrated into a TV or can be embodied by any hardware known in the art capable of performing the disclosed functions.

[0034] As shown in Figure 3, the DVB set top box communicates with the mobile terminal over any know communication link, such as a wired connection or a wireless RF or infra red link. One advantageous embodiment would employ Bluetooth for the communications between the set top box and the mobile terminal because it is an established standard and provides a ready made secure connection between the set top box and the mobile terminal. As previously discussed, the mobile terminal 70 is simply hardware device connected to the mobile network and programmed to perform the disclosed functions of the DRM system.

[0035] The process begins with the end user ordering protected DRM content. Lists of available content can be set up for browsing on the television via the DVB network or set top box or the mobile terminal itself via its user interface. In the case where the user browses for content on the mobile terminal, the mobile terminal can connect to servers at the DRM system, or from other sources, to receive data describing the available content choices. Alternately, the available content can be browsed and ordered via the voice telephone network.

[0036] In any case, once the user has selected a particular piece of content, the DRM System 30 is notified and begins to push the required DRM vouchers and software to the mobile terminal 70. The use of the mobile terminal in the ordering process enables the DVB content provider to make use of the mobile terminal billing network to charge for the content. In other words, if a user orders a pay per view movie the charge for that movie can be simply added to the users mobile phone bill.

[0037] With the content ordered the process of using the content beings. As shown in Figure 3, the set top box 41 receives, or has previously received and stored, the encrypted DVB content 1e and its associated ECMs 25. The set-top box, however, cannot use any of the encrypted DVB content 1e without the CSA control word contained in the ECM. However, the ECM must be decrypted with the appropriate service key to obtain the clear CSA control word. To do this the set top box 41 passes the ECM 25 to the mobile terminal 70 over the Bluetooth link 90. The Bluetooth link does not necessarily need to be protected at this stage because the ECM contains an encrypted CSA control word. Advantageously, many set top boxes already perform a similar function and send the received ECMs to a smart card for decryption. Thus, the set top boxes need only be redesigned to communicate with the mobile terminal instead of the smart card.

[0038] As described above, and shown in Figure 3, the mobile terminal 70 has received the Protected Application 36 and the DRM Voucher 35 from DRM System 30. The process for decrypting the CSA control word is as follows, preferably, the mobile terminal has a Mobile DRM Engine 72, which is hardware and/or software designed to perform secure processing and is resistant to tampering by individuals attempting to thwart the applied DRM. The DRM Engine runs the Protected Application 36, which has secure access to the UK 27. The protected application takes the DRM Voucher 35 and ECM 25 as input.

[0039] The DRM will then determine if the rights expressed in the DRM voucher allow the requested use, e.g. playing of DVB Content. If the requested use is allowed, the Protected Application uses the UK to decrypt 74 the SK contained in the EMM. The decrypted SK is then used to decrypt the CSA Control Word contained in the ECM to produce a clear CSA Control Word 10. The clear CSA Control Word is then sent back over the Bluetooth link to the set top box. Preferably, the transmission of the clear, i.e. unencrypted, CSA Control Word to the set top box occurs over a secure Bluetooth Link. Bluetooth Link Secure connections provide ready made authentication, authorization, and encryption (ciphering of plain text).

[0040] Distributing the Protected Application to practice the DRM System is particularly advantageous because the Protected Application can be tailored for the end user's specific mobile terminal and/or set top box thereby ensuring compatible operation for users regardless of the equipment employed.

[0041] Upon receipt of the decrypted CSA Control Word 10 the DVB set top box uses the CSA Control Word to perform DVB CSA Decryption 43. This generates clear DVB content 1c that can then be output to display 46 for use. Display 46 is merely a generic representation for use of the content. In practice the content could be music, software, etc., which would each be used on an appropriate device.

[0042] In alternative embodiments, the Protected Application may have a period of validity as expressed in DRM Voucher and the Protected Application may be made inoperable after the validity expires or the Protected Application may even be discarded, overwritten or deleted wholly or in part. In one embodiment of the invention the Protected Application that has been made inoperable may be re-activated with a response message from

the DRM system, wherein the re-activation message may be a DRM Voucher comprising another Protected Application .

[0043] Other embodiments could use the mobile phone network to receive location information from the network. The location of the mobile terminal can easily be determined down to cell level and the location data is available in the Visitor Location Register (VLR) in the network. The received location information may be used as part of the access control. For example, the DRM Voucher might contain geographic restrictions that can be applied using this feature.

[0044] Another advantageous embodiment would use the mobile terminal in connection with any near by device that receives DVB content. If a Bluetooth connection is used, the Bluetooth Service Discovery Protocol and Bluetooth pairing mechanism will provide a trust relationship that may be used for the necessary set top box identification. This functionality would allow a user to buy and use content at a friends house or other location.

[0045] In another advantageous embodiment, the DRM system can leverage the use of mobile terminals and implement the Open Mobile Alliance's (OMA) standard DRM infrastructure. The benefits of using OMA compliant mobile terminals to deliver EMMs and DRM rights are thus two fold. First, mobile terminals are a common piece of hardware owned by most individuals, therefore, the broadcaster can provide added services without deploying specialized hardware to all potential end users. Second, the use of mobile terminals also allows broadcasters to adopt standard mobile DRM systems like OMA thereby obviating the need to develop and maintain costly specialized systems. Both of these advantages lead to a system where an end users can employ standard equipment to obtain premium DVB content at the spur of the moment. This allows for a more marketable system

compared to a system where users must plan ahead and obtain special equipment to view premium content.

[0046] In general, OMA defines a software and hardware standard for mobile terminals. The OMA DRM standard allows compliant devices to implement and participate in a rights management system, including securely transmitting protected content and an executable application, such as a Java applet. The OMA compliant mobile terminal will then run the application, which contains the required UK and other security procedures necessary to ensure the protection of the protected content. In the present invention the protected content is simply the SK and the CSA control word rather than the actual usable media. Additional detailed descriptions of the OMA DRM system are documented in OMA published documents including OMA, DRM Content Format Version 1.0; OMA, Digital Rights Management Version 1.0; and OMA Rights Expression Language Version 1.0, which are all available at www.openmobilealliance.com and are hereby incorporated by reference.

[0047] In the context of the present invention, the DRM System would create Protected Applications and DRM Vouchers in accordance with the OMA standard. And the mobile terminal would be designed and programmed to follow the OMA standard when running the OMA application and following the DRM vouchers.

[0048] The many features and advantages of the present invention are apparent from the detailed specification, and thus, it is intended by the appended claims to cover all such features and advantages of the invention which fall within the true spirit and scope of the invention.

[0049] Furthermore, since numerous modifications and variations will readily occur to those skilled in the art, it is not desired that the present invention be limited to the exact

instruction and operation illustrated and described herein. Accordingly, all suitable modifications and equivalents that may be resorted to are intended to fall within the scope of the claims.